REMARKS

Claims 1 and 8 are amended, claims 7 and 13 are canceled, and claims 14-19 are added; as a result, claims 1-6, 8-12, and 14-19 are now pending in this application.

No new matter has been added by the amendments to claims 1 and 8. Support for the amendments to claims 1 and 8 is found throughout the specification, including but not limited to the specification at page 6, line 1 through page 7, line 21.

No new matter has been added through new claims 14-19. Support for new claims 14-19 is found throughout the specification, including but not limited to the specification at page 2, lines 23-27, page 3, lines 23 through page 4, lines 2, and in claims 1-6 as originally filed in the application.

§103 Rejection of the Claims

Claims 1-7 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Barrett's modular reduction method in view of Liardet et al. (U.S. Publication No. 2003/0044014A1).

Claims 8-13 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Applicant's Admitted Prior Art in view of Barrett's modular reduction method, and further in view of Liardet et al. (U.S. Publication No. 2003/0044014A1).

However, since a *prima facie* case of obviousness has not been established by the Final Office Action in each case, the Applicant respectfully traverses the grounds of rejection of these claims.

1) The Applicable Law:

The Examiner has the burden under 35 U.S.C. § 103 to establish a *prima facie* case of obviousness. *In re Fine*[1]. To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. *In re Royka*[2]. "All words in a claim must be considered in judging the patentability of that claim against the prior art." *In re*

[1] 837 F.2d 1071, 1074, 5 U.S.P.Q.2d (BNA) 1596, 1598 (Fed. Cir. 1988)
[2] 490 F.2d 981, 180 USPQ 580 (CCPA 1974).

Wilson[3]. Office personnel must rely on the applicant's disclosure to properly determine the meaning of the claims. *Markman v. Westview Instruments*[4].

2) Combining the Cited References Does Not Supply All Claimed Elements:

Amended independent claim 1 recites, in part, "applying said random error value to said estimated quotient value to obtain a randomized quotient q' = q – E." The Final Office Action states that Liardet teaches the above element of claim 1. Applicant respectfully disagrees with the Final Office Action and asserts that Liardet does not teach or suggest the above element.

In contrast, Liardet applies a random quantity "r" to an intermediate result $V2 = V1 \cdot a \bmod p$. The intermediate step and its randomized value V2', V2", V2"', etc. (depending on the embodiment) may be equivalent to the number "X" being reduced in claim 1 and not of the estimated quotient value q or its randomization q'. Moreover, Liardet does not teach randomizing of the quotient value that would be used in the modulo reduction operation itself, but only of the value of that is subject to the reduction. This is further illustrated in an example shown in Fig. 5 of Liardet where an intermediary value V2 is modified by adding a random multiple r of the modulus n, $V2' = V2 + r \cdot n$, the result B is recovered at a later step from V4' by a reduction modulo n, $B = V4' \bmod n$.

In another example, Fig. 6 of Liardet does not employ a modulo operation, but the intermediate result V2 is modified by adding a random value r, $V2" = V2 + r$, then after a subsequent multiplication by a factor q, $V3" + V2" \cdot q$, the result B can be recovered from V4" by a subtraction of the product $(q \cdot r)$, $B = V4" – q \cdot r$.

Moreover, Fig. 7 of Liardet uses two different moduli p and n, so where an intermediary result is modified by a random value r under a first modulus p, $V2"' = (V1 \cdot a + r) \bmod p$, and subsequently operated upon, $V3"' = V2"' \cdot q$, so that the result V5 can be recovered by a subtraction of the product $(q \cdot r)$, $V5 = V4"' – q \cdot r$, prior to reduction by the second modulus n.

Finally, the other embodiments (DSA-type) are basically similar, except that Fig. 8 randomly modifies the modulus q, $u2' = U1 + d \cdot t \bmod (q \cdot r)$, which necessitates a more complex recovery of the result $B = u3' = u2' \cdot k^{-1} \bmod q$. Thus, nowhere in Liardet is disclosed a

[3] 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970).
[4] 52 F.3d 967, 980, 34 USPQ2d 1321, 1320 (Fed. Cir.)(*en banc*), *aff'd*, U.S., 116 S.Ct. 1384 (1996).

quotient value q used for performing a modulo-reduction being randomized. Additionally, no combination of Barrett's modular reduction method and Liardet shows the above identified element of claim 1. For similar reasons, claim 8 is also not obvious over Barrett's modular reduction method and Liardet.

Furthermore, independent claims 1 and 8 have been amended to incorporate elements from claims 7 and 13 to recite in part, "wherein the random number generator has a specified error limit of one-half word, whereby $0 \leq E < (2^{w/2} - 1)$, with "w" being the word size of the computation unit in bits." The Final Office Action states that Barrett's method teaches and is shown by evidentiary evidence in Section 14.43 of The Handbook of Applied Cryptography. Applicant respectfully disagrees with the Final Office Action, and asserts that neither "The Handbook of Applied Cryptography," nor Liardet teaches or suggests the above element.

In contrast, Section 14.43 states, "By the division algorithm (Definition 2.82), there exists integers Q and R such that $x = Qm + R$ and $0 \leq R < m$. In step 1 of Algorithm 14.42, the following inequality is satisfied $Q - 2 \leq q_3 \leq Q$." Upon careful examination of the algorithm shown under Section 14.42 for Barrett modular reduction, the Applicant finds no disclosure of the above recited element of claims 1 and 8. No combination of Barrett's modular reduction method and Liardet "wherein the random number generator has a specified error limit of one-half word, whereby $0 \leq E < (2^{w/2} - 1)$, with "w" being the word size of the computation unit in bits."

Thus, since there is no evidence in the record to support all the claimed elements of claims 1 and 8, a *prima facie* case of obviousness has not been established with respect to these independent claims.

Furthermore, claims 2-6 depend either directly or indirectly from independent claim 1. Claims 9-12 depend either directly or indirectly from independent claim 8. Therefore, these dependent claims inherit the elements of their respective base claims, and are not obvious in view of Barrett's modular reduction method and Liardet for at least the reasons stated above with respect to independent claims 1 and 8. Applicants therefore respectfully request reconsideration and the withdrawal of the rejection of claims 1-6 and 8-12.

New Claims 14-19

Applicant respectfully submits that, for at least the reasons stated above with respect to claims 1-6, new claims 14-19 are distinguishable over any of the documents cited in the Final Office Action, in any proposed combination of documents used in the rejections of claims 1-7 and 8-13 in the Final Office Action.

Applicant respectfully requests consideration and allowance of new claims 14-19.

Reservation of Rights

In the interest of clarity and brevity, Applicant may not have equally addressed every assertion made in the Final Office Action, however, this does not constitute any admission or acquiescence. Applicant reserves all rights not exercised in connection with this response, such as the right to challenge or rebut any tacit or explicit characterization of any reference or of any of the present claims, the right to challenge or rebut any asserted factual or legal basis of any of the rejections, the right to swear behind any cited reference such as provided under 37 C.F.R. § 1.131 or otherwise, or the right to assert co-ownership of any cited reference. Applicant does not admit that any of the cited references or any other references of record are relevant to the present claims, or that they constitute prior art. To the extent that any rejection or assertion is based upon the Examiner's personal knowledge, rather than any objective evidence of record as manifested by a cited prior art reference, Applicant timely objects to such reliance on Official Notice, and reserves all rights to request that the Examiner provide a reference or affidavit in support of such assertion, as required by MPEP § 2144.03. Applicant reserves all rights to pursue any cancelled claims in a subsequent patent application claiming the benefit of priority of the present patent application, and to request rejoinder of any withdrawn claim, as required by MPEP § 821.04.

CONCLUSION

Applicant respectfully submits that the claims are in condition for allowance and notification to that effect is earnestly requested. The Examiner is invited to telephone Applicant's attorney (612) 371-2132 to facilitate prosecution of this application.

If necessary, please charge any additional fees or credit overpayment to Deposit Account No. 19-0743.

Respectfully submitted,

SCHWEGMAN, LUNDBERG & WOESSNER, P.A.
P.O. Box 2938
Minneapolis, MN 55402
(612) 371-2132

Date APRIL 14/2008

By Robt B Madden
Robert B. Madden
Reg. No. 57,521

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being filed using the USPTO's electronic filing system EFS-Web, and is addressed to: Mail Stop RCE, Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on this 14 day of April 2008.

Name

Signature